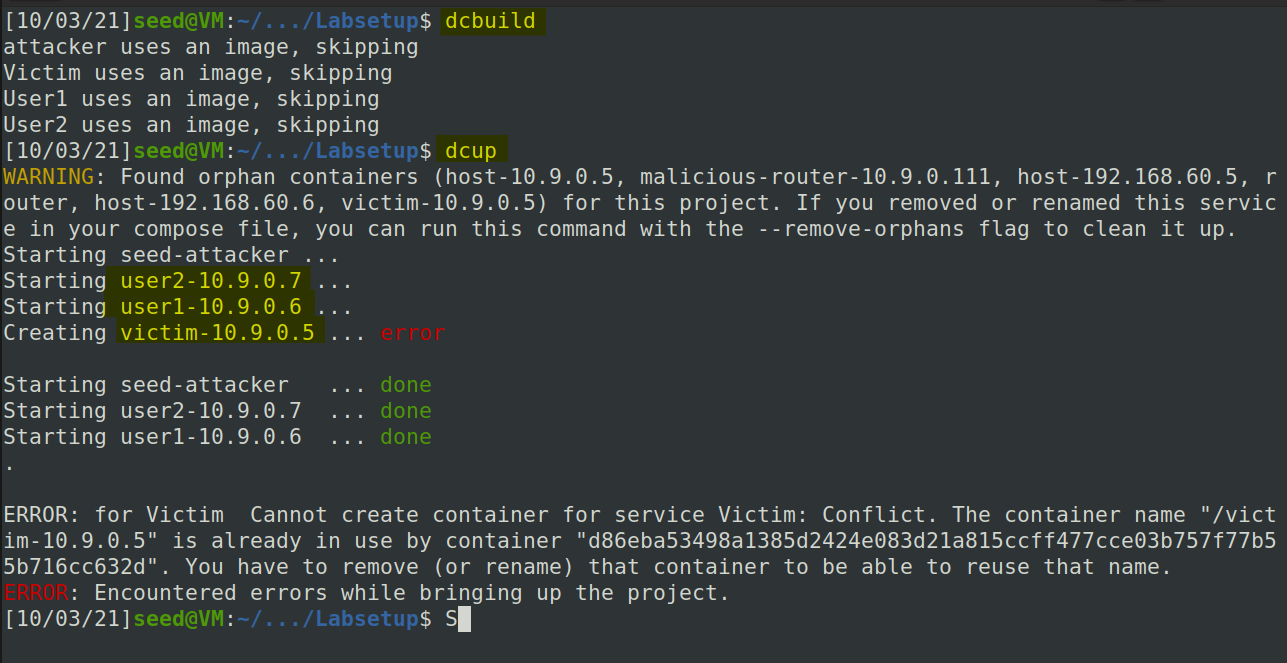
Lab-5 Report: TCP Attack

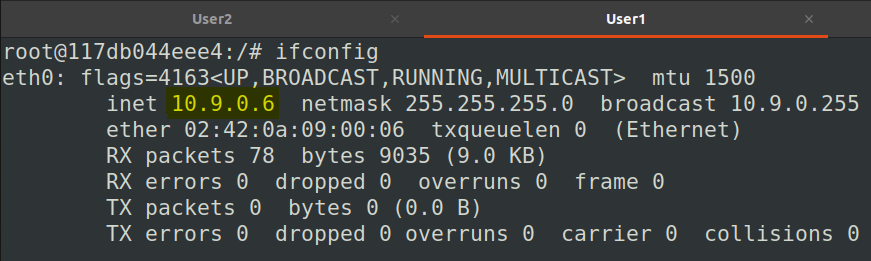
Shrikant Kale - 700727822

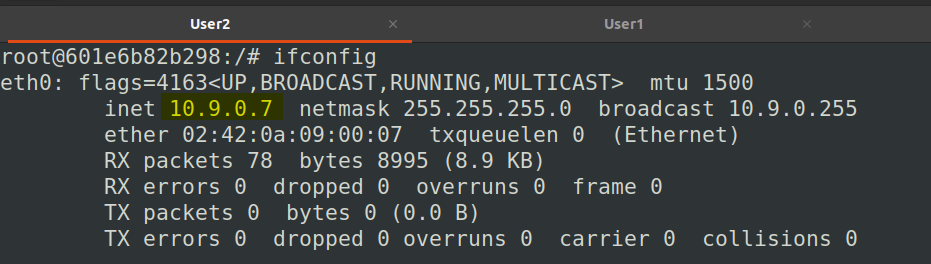
**Lab Environment Setup**

* Created Lab environment using docker containers.
* To execute docker container, I have used docker-compose commands.
  + dcbuild (docker-compose build) – to build the docker container image
  + dcup (docker-compose up) – to run the docker container
  + dcdown (docker-compose down) – to shut down the container



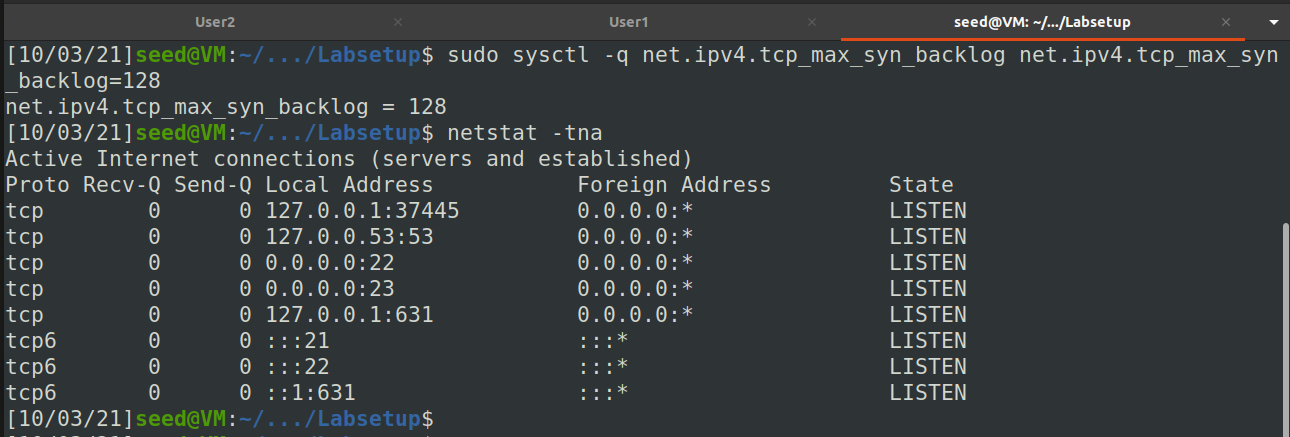
Network Setup:

****

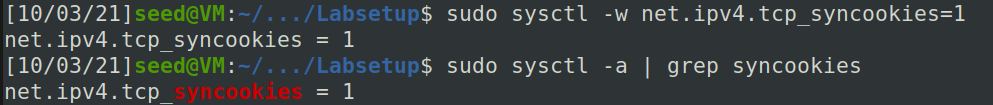


1. **Task 1) SYN Flooding Attack**

As seen in the screenshot, the victim’s queue size is 128. We also see the current open ports that are awaiting connections (LISTEN stage.) If a port had a half-open connection (only SYN received and no ACK from the client), then the state would’ve been SYN\_RECV. If the 3-way handshake completes, the state changes to ESTABLISHED.

****

**SYN Cookie Countermeasure:** By default, Ubuntu’s SYN flooding countermeasure is turned on. This mechanism is called SYN cookie.

****